UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/621,059	07/21/2000	Dennis K. Branstad	NAI1P079/99.122.01	4287

28875 7590 03/04/2004

SILICON VALLEY INTELLECTUAL PROPERTY GROUP
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
HO, THOMAS M	

ART UNIT	PAPER NUMBER
2134	11

DATE MAILED: 03/04/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/621,059	BRANSTAD ET AL.	
	Examiner	Art Unit	
	Thomas M Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *21 July 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The Amendment of 01-22-01 has been received and entered.

2. Claims 1-16 are pending.

Double Patenting

3. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claim 1 rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 1 of U.S. Patent No. 09/621056 and claim 1 of Application No. 09/621057. Although the conflicting claims are not identical, they are not patentably distinct from each other because the two claims of 09/621059 and 09/621056 read on each other.

Claim 1 of 09/621059 reads:

A method for generating an authentication tag for a message, comprising:

- Processing a portion of a message using a first function to produce an interim output.
- Processing the interim output using a second function to produce the authentication tag.

Claim 1 of 09/621056 reads:

A method for generating an authentication tag for a message that can be used for error correction processing comprising:

- Processing a portion of the message using a reversible first function to produce an intermediate result.
- Processing the intermediate result with a second function to produce the authentication tag.

While Claim 1 of 09/621059 recites processing a portion of a message using a first function and Claim 1 of 09/621059 recites a "reversible first function", it is understood that a reversible first function is still a function. Additionally the method for generating an authentication tag that can be used for error correction (09/621056) is still a method for generating an

authentication tag (09/621059). Claim 1 of 09/621059 is then broader than Claim 1 of 09/621056 and is not patentably distinct over 09/621056.

It would have been obvious to one of ordinary skill in the art at the time of invention to process a message using a function in Claim 1 of 09/621059 to generate an authentication tag in view of Claim 1 of 09/621056 since Claim 1 of 09/621059 is inherent to Claim 1 of 09/621056.

Claim 1 of 09/621057 reads:

An authentication system, comprising:

- A plurality of inner functions that are operative on a respective plurality of collections of message parts to produce a plurality of intermediate outputs
- An outer function that is operative on said plurality of intermediate outputs to generate an authentication tag.

Claim 1 of 09/621059 is obvious over claim 1 of 09/621057, the only difference being that claim 1 of 09/621057 claims a plurality of these inner function, and consequently a plurality of inputs and outputs.

It would have been obvious to one of ordinary skill in the art at the time of invention to apply the authentication system computation of claim 1 (09/621057) only once, to produce an authentication tag from a "portion of a message using a reversible first function to produce an intermediate result", for the advantage of producing a singular authentication tag when only one is needed rather than a plurality of them.

Claim 4 is rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 4 of U.S. Patent No. 09/621057 and claim 3 of U.S. Patent No. 09/621057. Although the conflicting claims are not identical, they are not patentably distinct from each other because the two claims of 09/621059 and 09/621057 read on each other.

Claim 4 of 09/621059 reads:

A method according to claim 1, further comprising partitioning the message into regions, each region including a number of message parts, and providing one message part from each region as input to said first function.

Claim 4 of 09/621057 reads:

The system of claim 1, further comprising a first bin for storage of said first collection of message parts, and a second bin for storage of said second collection of message parts.

Claim 4 of 09/621059 is obvious over claim 4 of 09/621057 with the only difference being Claim 4 of 09/621059 specifying an undisclosed number of bins for storage. The "bins" as understood from claim 4 of 09/621057 are understood as being inputs to the two inner functions for a method creating an authentication tag.

It would have been obvious to one of ordinary skill in the art at the time of invention to create partitions of regions of message parts in Claim 4 of 09/621059 from the collections of message parts in Claim 4 of 09/621057, by generalizing the number of bins to any number which added flexibility and increased speed in a parallel computation of the inner functions.

Claims 3 of 09/621057 reads:

The system of claim 1, wherein said plurality of collections of message parts are distinct.

Claim 4 of 09/621059 reads on claim 3 of 09/621057 because, being able to provide only one message part from each region in claim 4 of 09/621059 would imply a certain distinctness, or the ability to distinguish one region, or collection of message parts from another, enough so that it is possible to only provide a single message part from each region.

It would have been obvious to one of ordinary skill in the art at the time of invention to process a message using a function in Claim 4 of 09/621059 to generate distinct collections of message parts in view of Claim 3 of 09/621057 since Claim 3 of 09/621057 is inherent to Claim 4 of 09/621059.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-16 are rejected under 35 U.S.C. 102(a) as being anticipated by Balenson et al.

In reference to claim 1:

Balenson et al. (Figure 4, page 19) discloses a method for generating an authentication tag for a message, comprising:

- Processing a portion of the message using a first function to produce an interim output, where the first function is the inner function which produces an interim output.
- Processing the interim output using a second function to produce the authentication tag, where the second function is the outer function, and the result is an Authentication Tag.

In reference to claim 2:

Balenson et al. (Section 2.4.3 Probabilistic Authentication, p. 23-24) discloses a method according, wherein the message includes a number of message parts, and wherein the portion of the message processed is selected by using a pseudorandom probabilistic function to determine whether each message part is provided as input to said first function, where the probabilistic function determines whether each message part is provided as input to the first function

In reference to claim 3:

Balenson et al. (P.14 ACSA session parameters) discloses a method wherein said message parts are 64-bit words, where the data word size are the message parts, and depending on the hardware used, can be 64 bits (32 in the case of the Pentium).

In reference to claim 4:

Balenson et al. discloses a method further comprising partitioning the message into regions, each region including a number of message parts, and providing one message part from each region as input to said first function, where the message regions are packets (section 2.4.3 page 23), and the message region contains message parts which are data words, and (Section 3.3.2, page 31) discloses an embodiment wherein the computation is performed using all the data words of the message.

In reference to claim 5:

Balenson et al. discloses a method wherein the message includes a number of message parts, and wherein the portion of the message processed is selected by:

- Defining a message selection percentage p, where defining a message selection percentage p is inherent in to defining a probability that a particular word is to be included in the computation of the authentication tag. If one defines the probability that a section of the message to be included is p, then inherently that message p is included (100 * p) % of the time.
- Using a pseudorandom probabilistic function, uniform over an interval [1,2L], where L = 1/p and p is a message selection percentage, to determine offsets between message parts which are provided as input to said first function, where determining the offsets between message parts is inherent to defining p as a message selection percentage. The computation of selecting a message part to be used in the Authentication Tag with probability p serves to define which message parts are to be used. Once the message parts to be used have been decided, then inherently one thereby knows the offsets

between the message parts, since the offsets are simply the consecutive message parts NOT included in the computation.

In reference to claim 6:

Balenson et al. (Page 19, Figure 4) discloses a method wherein said first function is a keyed hash function.

In reference to claim 7:

Balenson et al. (Section A.2, page 36-43) discloses a method, wherein the cryptographic hash function is one of an MD4 hashing function, a bucket hashing function, a multilinear modular hashing function, a cyclic redundancy code-based hashing function, and an alternative hashing algorithm, where disclosed are MD4, Bucket Hashing, and a cryptographic CRC function.

In reference to claim 8:

Balenson et al. (Page 19, Figure 4) discloses a method wherein the portion of the message processed is selected by truncating the message, where the message being processed is truncated at the output of the HMAC-SHA-1-96.

Claim 9 is rejected for the same reasons as claim 1.

Claim 10 is rejected for the same reasons as claim 2.

Claim 11 is rejected for the same reasons as claim 3.

Claim 12 is rejected for the same reasons as claim 4.

Claim 13 is rejected for the same reasons as claim 5.

Claim 14 is rejected for the same reasons as claim 6.

Claim 15 is rejected for the same reasons as claim 7.

Claim 16 is rejected for the same reasons as claim 8.

6. Claims 1, 9 are rejected under 35 U.S.C. 102(b) as being anticipated by Bellare et al.

In reference to claim 1:

Bellare et al. (The Nested Construction, NMAC, page 9) discloses a method for generating an authentication tag for a message, comprising:

- Processing a portion of the message using a first function to produce an interim output, where the interim output is $F_{k2}(x)$.

- Processing the interim output using a second function to produce the authentication tag, and the interim output $F_{k2}(x)$ is processed as $F_{k1}(F_{k2}(x))$ to generate an authentication tag.

Claim 9 is rejected for the same reasons as claim 1.

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas M Ho whose telephone number is (703)305-8029. The examiner can normally be reached on M-F from 8:30am – 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached at (703)308-4789. The fax phone numbers for the organization where this application or proceeding is assigned are (703)746-7239 for regular communications and (703)746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)306-5484.

TMH

February 12th 2003

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100